REMARKS/ARGUMENTS

Prior to this amendment claims 1-9 were pending. In this amendment, claims 1-2 and 8-9 are amended. Claims 10-15 are added. Thus, after entry of this amendment, claims 1-15 will be pending.

Rejection under 35 U.S.C. § 101

Claims 1-9 were rejected under 35 U.S.C. 101 because the claimed invention is based on non-statutory subject matter and directed towards an abstract idea of a mathematical algorithm. Claim 1 recites "*determining the number of points on the elliptic curve*." The number of points on a particular elliptic curve is a tangible result that is useful for many purposes. Accordingly, Applicant requests the withdrawal of the §101 rejection in light of amended claims 1-9.

Arguments for Rejection-35 U.S.C. § 103(a)

Claims 1-9 have been rejected under 35 USC §103(a) as being obvious over Hoffstein et al. (U.S. Patent No. 7,031,468) in view of Gressel et al. (U.S. Patent No. 6,748,410) and in further view of Penner (U.S. Patent No. 7,158,569). Applicant respectfully traverses this rejection.

Claims 1-11

Claim 1 is allowable over the cited references, either alone or in combination, as those references fail to teach or suggest all the elements of claim 1. For example, claim 1 recites:

> *determining a number of points on the elliptic curve, wherein the determining includes solving a lifted Frobenius equation to a full precision by using first and second parts with a reduced precision.*

Hoffstein is directed to computing powers of a number, e.g. A^k. *See Hoffstein*, col. 1 lines 23-27. One method described is "writing k as a sum of powers of the p-power Frobenius map on the group of points $E(GF(p^m))$ on an elliptic curve E defined over the finite field GF(p)." *Id.*, col. 1 lines 56-59. The use of the Frobenius map is to multiply points on the curve, and not to determine a number of points on the curve. In contrast, claim 1 recites "*determining a number of points on the elliptic curve*."

Additionally, the Frobenius map is not solving a Frobenius equation, particularly a lifted Frobenius equation. These are two difference mathematical entities. Furthermore, the multiplication involves finite elements having only a single precision, and thus both a full precision and a reduced precision, as recited in claim 1, are not taught or suggested.

Gressel also only mentions performing multiplications on an elliptic curve and not determining a number of points on the curve. *See Gressel*, col. 1 lines 49-53. Penner does not mention an elliptic curve at all. Neither Gressel or Penner mention a Frobenius equation, and particularly not a lifted Frobenius equation. Note that Penner does not refer to a canonical lift or any similar object although the Office Action cites as such on Page 5. Penner does not even use the word "lift." Thus, these reference do not make up for the above-mentioned deficiencies of Hoffstein.

Moreover, besides not mentioning or even being related to solving a Frobenius equation, none of the cited reference mention the steps of solving the equation as recited in claim 1. The Office Action does not cite where any of the steps are actually mentioned in any of the references, but simply asserts that the combination teaches them without any specification of where the steps are actually taught. Only vague assertions of similar words being used are provided.

For at least these reasons, claim 1 is allowable over the cited references. As claim 1 is allowable, claims 2-11 which depend therefrom are also allowable for at least the same rationale.

Claim 10

In addition to being allowable for the same rationale as claim 1, claim 10 is allowable for additional reasons. For example, claim 5 recites " *based on the number of points, identifying the elliptic curve as a secure elliptic curve for generating a cryptographic key."*

The cited references also does not mention identifying a secure elliptic curve, particularly not *"based on the number of points,"* as recited in claim 10. As mentioned above, not one of the references teach or suggest determining a number of points on the elliptic curve, and not one of the references teaches or suggests using the number of points to identify an

elliptic curve as secure. For at least this additional reason, claim 10 is allowable over the cited references.

Claims 12-15

Applicants submit that independent claims 12 and 14 should be allowable for reasons mentioned with respect to claim 1. As claim 12 is allowable, dependent claim 13 is allowable for at least the same rationale. As claim 14 is allowable, dependent claim 15 is allowable for at least the same rationale. Exemplary support for these claims can be found at least in paragraphs 76-80.

CONCLUSION

In view of the foregoing, Applicants believe all claims as amended and now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at (415) 576-0200.

Respectfully submitted,

/David B. Raczkowski/

David B. Raczkowski
Reg. No. 52,145

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 925-472-5000
Fax: 415-576-0300
DBR/scz
61205933 v1